EP2004/8574 D2646

Europäisches Patentamt | European Patent Office | Office européen des brevets

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. | Patent application No. | Demande de brevet n°

03017348.8

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Anmeldung Nr:
Application no.: 03017348.8
Demande no:

Anmeldetag:
Date of filing: 31.07.03
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

T-Mobile Deutschland GmbH
Landgrabenweg 151
53227 Bonn
ALLEMAGNE

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Transparent access authentication for IMS in 2G and 2.5G mobile access networks

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

H04Q7/38

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL
PT RO SE SI SK TR LI

Transparent Access Authentication for IMS in 2G and 2.5G Mobile Access Networks

Abstract

In standardisation of UMTS Rel.5 comprehensive means are foreseen to perform authentication on the application layer with no need to interwork with the underlying radio and transport networks. The mechanisms are based on the assumption that a specific environment is prepared for deployment of IMS. It includes the use of ISIM application, which in turn requires Rel.99UICC's in the connected end devices to handle the AKA.

In case of deployment of IMS and IMS based services in a network environment which is characterised by the use of SIM cards, the standardised authentication mechanism will not be applicable.

The present paper describes a method for application layer authentication of subscribers, connected to the authenticating network domain by a 2G or 2.5G GPRS core network or a 3G UMTS network. The authentication will be based on data which is assembled by the network layer during establishment of a PDP context in GPRS networks. This information is secured by standard SIM card application. As the same mechanisms are used for authentication in 3G networks, the further described mechanism would also be applicable there. No standard would be touched in any way while using a 2G or 2.5G access network, because no authentication on application layer is foreseen in the standard. For UMTS Rel.5 standards and following, the standard foresees specific methods. The use of the further described method would be possible, although the standardised authentication mechanism needs to be switched off. Switching

off the standardised authentication mechanism could be interpreted as standard sensitive, but subsequent use of the further described mechanism would be standard compliant again.

Finally a migration path to UMTS Rel.5 standardised authentication and the concept for parallel use of bot mechanisms will be described.

Description

During PDP context establishment the SGSN is authenticating the subscriber using the A3/A8 algorithm based on the end devices SIM card in case of GSM and 2.5G GPRS and EDGE access network. In 3G networks authentication is done based on XXXXX.

The GGSN receives a context creation request and queries a Radius server to get an IP address assigned for the particular PDP context. Within the context the Radius server receives the MSISDN and/or the IMSI of the subscriber. So in the database of the Radius server we find for each PDP context a pair of IP address and IMSI/MSISDN. Based on the TEID the GGSN filters all packets running through the PDP context once established, for the correct IP source address. This means the GGSN checks matching TEID/IP address pairs, thus preventing falsification of source addresses and so called "IP spoofing" for the complete lifecycle of the PDP context.

In the application domain a database exists that stores all PubID's the subscriber is using in the domain, referring it to his PrivID, which is unique in the respective application domain. The PrivID is correlated with an MSISDN and/or IMSI. In the request the user gives his PrivID for registration. Upon receiving the registration request, the registration

proxy queries the database containing the subscribers ID's (both public and private) together with the MSISDN/IMSI. This data is stored in a table on the proxy platform.
Subsequently the proxy queries the database of the Radius server in order to get the assigned IP address of that session and the IMSI/MSISDN already authenticated by the HLR. The authentication of the HLR guarantees further that the IP address can be considered to be authenticated as well. Also this information is stored in the table on the proxy platform.

Now the proxy starts the authentication procedure.

First it checks IMSI/MSISDN from Radius server database and application domain database for match. If the pairs are not matching the subscriber has tried to register with an incorrect PrivID, which is not correlated with his IMSI/MSISDN, if the pairs are matching the next step is performed.

Second step is checking the subscribers IP address in the IP network layer, meaning in the IP packet overhead field for source address for match with the IP address assigned by the Radius server. As the IP address was assigned to an IMSI/MSISDN-authenticated session, also the IP address can be considered as authenticated.
If the pairs are not matching, the subscriber used an incorrect IP address, if the pairs are matching the subsequent step is performed.

The proxy parses the application layer for IP addresses given in the headers of e. g. SIP registration message, SDP message bodies, etc and checks for match with the IP address in,

which was already checked for match with the IP address assigned by the Radius server. If the pairs are not matching the subscriber used incorrect signalling information, e. g. response addresses, etc. If the pairs are matching, the session setup can be considered as authenticated.

In all subsequent messages arriving at the proxy, it checks for match of IP address in the IP packet overhead field for source address with that in the application layer protocol header fields and verifies the matching pairs against the IP address assigned by the Radius server.
If PubID's are used in the following session, the PubID's are checked against the PrivID which was stored in a table on the proxy platform after querying the application domains database.

The described functionality gives the network operator the opportunity to run authentication transparently to the end device, without requiring proprietary extensions and functions on network or client side. In case of SIP based signalling, the migration to fully standard compliant UMTS Rel.5 mechanisms and a strategy for parallel operation is necessary, this will be described now.

As the IMS domain as standardised for UMTS Rel.5 will include it's own authentication mechanism, it is necessary to support a scenario where the subscribers are migrating to ISIM enabled end devices. To exploit the benefits of the standardised authentication mechanism, both mechanisms have to be supported in parallel.
This is done by an additional function that checks each incoming signalling message, first for the protocol, if it's any other protocol than SIP, the session is routed to the

proxy. The same routing decision is taken if the message is based on SIP, but the client does not support standardised UMTS Rel.5 authentication. If the client does support standardised authentication method, e. g. is ISIM enabled, the message is routed to the standard compliant P-CSCF. First trigger for routing decisions is the protocol type, as described above. Further triggers could be the key exchange mechanism used for setting up the secured connection between UE and P-CSCF (if the end device is starting key agreement, it can be considered as standard compliant and the request is routed to the P-CSCF), or other elements included in the UMTS Rel.5 header as well as any private extension, which is, however, possible but not necessary. If trigger points available in signalling should be insufficient, also database lookups can be used to base routing decisions on.

Abbreviations

AKA	authentication and key agreement
UICC	UMTS IC Card
ISIM	IMS SIM
SIM (card)	(GSM) Subscriber Identity Module (card)
UMTS	universal mobile telecommunication system
IMS	IP multimedia subsystem
2G	second generation (e. g. GSM)
2.5G	second and half generation (e. g. GPRS, EDGE)
3G	third generation (e. g. UMTS)
P-CSCF	Proxy-Call-State-Control-Function
UE	User Equipment
IMS	IP Multimedia Subsystem

Claims

1. Method for application layer authentication of subscribers, connected to the authenticating network domain by a 2G or 2.5G GPRS core network or a 3G UMTS network, characterised by using data which are assembled by the network layer during establishment of a PDP context in GPRS networks.

2. System of units in a mobile telecommunication network, characterised that at least a first authentication unit is connected via a data line to a second unit which assembles data according to the method of claim 1.